

**REMARKS**

This responds to the Office Action dated October 6, 2005.

Claims 1, 17, and 35 are amended, claim 34 is cancelled; as a result, claims 1-33 and 35-37 are now pending in this application. The amendments to the claims are consistent with the original filed specification and Applicant does not believe that the amendments necessitate a new search. Accordingly, Applicant respectfully requests that the amendments be entered.

**§101 Rejection of the Claims**

Claim 34 was rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Although Applicant continues to disagree with the Examiner's assessment of signal claims, Applicant has cancelled claim 34. However, Applicant reserves the right to reintroduce the subject matter of this claim in a later continuation and reserves the right to continue to object to the Examiner's rationale for rejecting the signal-based claim.

**§102 Rejection of the Claims**

Claims 34 was rejected under 35 U.S.C. § 102(e) for anticipation by Gressel (U.S. 6,311,272). This rejection is no longer appropriate and does not exist in view of the fact that the Applicant has cancelled claim 34.

**§103 Rejection of the Claims**

Claims 1-5, 8, 13, 15-21, 25, 27-30 and 35 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hoke et al. (U.S. 6,701,437) in view of Schneier (Applied Cryptography) and Shimbo et al. (U.S. 6,092,191). It is of course fundamental that in order to sustain an obviousness rejection that each and every element or step in the rejected claims must be taught or suggested in the proposed combination of references.

At the outset, Applicant would like to reiterate and incorporate by reference the objections that Applicant raised with respect to combining Hoke and Shimbo. Applicant does not believe that a small portion of one reference can be taken in isolation from its remaining teachings and used out of context from its teachings to provide motivation and compatibility

between references that are being combined. One of ordinary skill in the art would have been reading the teachings in the context of the entire disclosure and one of ordinary skill in the art would not have used portions out of context unless Applicant's disclosure was read and comprehended in order to provide a motivation to do so. If this was done, then it is improper hindsight and is impermissible. Therefore, Applicant continues to respectfully disagree with the manner in which the Examiner asserts that Hoke and Shimbo were combined in the first instance.

Furthermore and with respect to Shimbo, the Examiner asserts that if Schneier is combined with Shimbo, a data structure can be indexed to provide cryptographic information in a manner similar to what is claimed in Applicant's independent claims 1, 17, and 35. Applicant respectfully disagrees with this conclusion because in Shimbo the cryptographic information (identified as a key) is acquired from a data structure based on three criteria, namely a source address, a destination address, and a connection id. See Shimbo, FIG. 6 and related discussion in the specification.

Notice that any particular source address (*e.g.*, H1) can occur multiple times within the data structure as can a destination address (*e.g.*, H2). Notice also that the key is dependent on a particular connection or session id. This is not the case with Applicant's amended independent claims, where the data structure is accessed only after an entity name is decrypted from a connection id and the cryptographic information obtained is independent of any particular connection.

So, the proposed combination of Schneier and Shimbo still fails to teach using a single entity name to acquire cryptographic information that is then used independent of any particular connection or session. In fact, the data structure of Shimbo is dependent on connection id and uses three identifiers, namely the connection id, the source address, and the destination address.

Moreover, the reference to Kerberos and its techniques of Schneier is misplaced because tickets and encryption of Kerberos is good for only single sessions and single clients possessing valid tickets and authenticators. The cryptographic information is not independent of a session or connection and it is specific to a holder of a ticket and specific to a session connection. Conversely, Applicant's independent claims permit any trusted party with access to the shared secret value to acquire cryptographic information by decoding a connection id to acquire an entity name and then using that entity name to access a data structure having the cryptographic

information; and the cryptographic information is independent of any particular session or connection. Kerberos cannot achieve this and its teachings specifically prohibit this scenario, since by definition an authenticator is only used once and is only available on a per session basis. See Schneier, page 568, paragraphs 2-4.

Accordingly, Applicant submits that the proposed combination of references, even if permissible, fails to teach each and every limitation of Applicant's amended independent claims. Therefore, the rejections should be withdrawn and the claims allowed. Applicant respectfully requests an indication of the same.

Claims 6, 9-12, 14, 22-24, 26, 31-33 and 36-37 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hoke et al. in view of Schneier and Shimbo et al. as applied to claim 1 above, and further in view of Demers et al. (5,857,023). Claims 6, 9-12, and 14 are dependent from independent claim 1, claims 22-24, 26, and 31-33 are dependent from independent claim 17, and claims 36-37 are dependent from independent claim 35; therefore, for the remarks presented above with respect to claims 1, 17, and 35, the rejection of the claims 9-10, 14, 26, 31-33, and 36-37 should be withdrawn and these claims allowed. Applicant respectfully requests an indication of the same.

### CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney (513) 942-0224 to facilitate prosecution of this application.

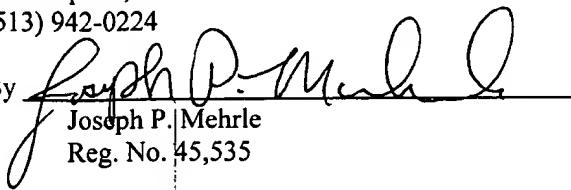
If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

HILARIE K. ORMAN

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.  
P.O. Box 2938  
Minneapolis, MN 55402  
(513) 942-0224

Date 12-06-05  
By   
Joseph P. Mehrle  
Reg. No. 45,535

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop AF, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 6 day of December, 2005.

Peter Rabuffoni  
Name

  
Signature